IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

FEE TRANSMITTAL SHEET FOR
CONTINUATION PATENT APPLICATION UNDER § 1.53(b)

Transmitted herewith for filing is the **continuation patent application under § 1.53(b)** of:

Inventor: Geoffrey b. Rhoads

For: SECURITY DOCUMENT WITH STEGANOGRAPHICALLY-ENCODED
AUTHENTICATION DATA

The fee is calculated below:

CLAIMS AS FILED					
For	Number Filed		Number Extra	Rate	Basic Fee $760.00
Total claims	7	-20	0	x $18.00 =	
Independent Claims	1	-3	0	x 78.00 =	0
TOTAL FILING FEE					$760.00

DATE OF DEPOSIT: November 23, 1998

[X] The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this application and recording any assignment filed herewith, or credit over-payment, to Account No. 02-4550. A copy of this sheet is enclosed.

[X] A check in the amount of $ 760.00 to cover [x] filing fee is enclosed.

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
cc: Geoffrey B. Rhoads (w/encl.)
     Bruce Davis (w/o encl.)
     Scott Carr (w/o encl.)
     Docketing Secretary

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

By_____
   William Y. Conwell
   Registration No. 31,943

FORM 4-1A

11/23/98

Please type a plus sign (+) inside this box → [+]

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	4830-51475/WYC
First Inventor or Application Identifier	Geoffrey B. Rhoads
Title	SECURITY DOCUMENT WITH STEGANOGRAPHICALLY-ENCODED AUTHENTICATION DATA
Express Mail Label No.	EL121478880US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original, and a duplicate for fee processing)

2. [X] Specification [Total Pages 13]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) (35 U.S.C. 113) [Total Sheets 5]

4. Oath or Declaration [Total Pages 2]
   a. [ ] Newly executed (original or copy)
   b. [X] Copy from a prior application (37 C.F.R. § 1.63(d))
   (for continuation/divisional with Box 17 completed)
   [Note Box 5 below]
   i. [ ] DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

5. [X] Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered to be part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. [ ] Microfiche Computer Program (Appendix)

7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (Identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. [ ] Assignment Papers (cover sheet & document(s))
9. [ ] 37 C.F.R.§3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
10. [ ] English Translation Document (if applicable)
11. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
12. [ ] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. [ ] * Small Entity Statement(s) (PTO/SB/09-12) [ ] Statement filed in prior application, Status still proper and desired
15. [ ] Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. [ ] Other: ....
....
* A new statement is required to be entitled to pay small entity fees, except where one has been filed in a prior application and is being relied upon.

17. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:
[X] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: 08/763,847
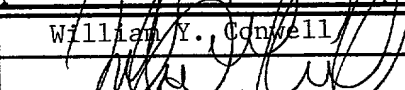Prior application information: Examiner Tadayon Group / Art Unit: 2721

18. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label (Insert Customer No. or Attach bar code label here) or [ ] Correspondence address below

Name	William Y. Conwell
	Klarquist Sparkman Campbell Leigh & Whinston, LLP
Address	One World Trade Center, Suite 1600
	121 S.W. Salmon Street

City	Portland	State	OR	Zip Code	97204
Country	USA	Telephone	503-226-7391	Fax	503-228-9446

Name (Print/Type)	William Y. Conwell	Registration No. (Attorney/Agent)	31,943
Signature		Date	11/23/98

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

SECURITY DOCUMENT WITH STEGANOGRAPHICALLY-ENCODED
AUTHENTICATION DATA

Related Application Data

This application is a continuation of application No. 08/763,847, filed December 4, 1996, allowed, which is a continuation of application No. 08/512,993, filed August 9, 1995, now abandoned, which is a continuation-in-part of each of applications 08/436,098 (now Patent 5,636,292), 08/436,099 (now Patent 5,710,834), 08/436,102 (now Patent 5,748,783), 08/436,134 (now Patent 5,748,763), and 08/438,159 (co-pending), each filed May 8, 1995. This application is also a continuation-in-part of copending application 08/327,426, filed October 21, 1994, which is a continuation-in-part of application 08/215,289, filed March 17, 1994, now abandoned, which is a continuation-in-part of application 08/154,866, filed November 18, 1993, now abandoned.

Technical Field

The present invention relates to the field of photograph-based identification systems.

Background and Summary of The Invention

The use of photograph-based identification ("photo ID") systems is pervasive. Drivers' licenses, passports, visas, government employee cards, immigration documents, and now, more frequently, credit cards and cash transaction cards carry a photograph of the card bearer for identification purposes. Many industries require that their employees carry photo ID on the job.

Fraudulent use of photo ID systems may occur where, for example, an otherwise legitimate passport is modified such that the original photograph is swapped with that of another person, thereby enabling the other person to travel, at least temporarily, under the guise of the original passport holder.

Even in the absence of photograph swapping or alteration, it is oftentimes difficult to confirm by inspection that the individual depicted in the photograph of the identification card is indeed the bearer of the card.

One aspect of this invention provides for enhanced security and certainty in the use of photo ID documents.

An illustrative embodiment of the present invention is a method of correlating, with a photograph, information about an individual whose image appears in the photograph. The method includes steganographically encoding multi-bit information into the photograph. This encoding serves to add noise to the photograph – noise that is not generally perceptible as a representation of the multi-bit information except by computer analysis. (The encoded photograph appears to convey only an image of the individual to viewers of the photograph.) Sometime after encoding, the multi-bit information is decoded. Finally, some sort of authentication decision about the individual is made, based at least in part on the multi-bit information decoded from the photograph.

Another illustrative embodiment of the present invention is a substrate (e.g. a card, or a page from a magazine) with a photograph. The photograph is steganographically encoded with multi-bit data related to the photograph. This data is manifested as a slight snow effect that is not generally perceptible as a representation of the multi-bit data except by computer analysis. The multi-bit data can serve various purposes (e.g. identify an owner of the photograph; serve as a serial number index into a database, etc.).

The foregoing and other aspects of the invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description Of The Drawings

Figs. 1-5 detail aspects of a security card according to one embodiment of the present invention.

Fig. 6 is a diagram of a photographic identification document or security card with which the security system aspect of the present invention may be applied.

<u>Detailed Description of Preferred Embodiments</u>

To provide a comprehensive disclosure without unduly lengthening the present specification, applicant incorporates by reference the Drawings and Detailed Description (only) from applicant's patent 5,710,834.

5

<u>PLASTIC CREDIT AND DEBIT CARD SYSTEMS BASED ON THE PRINCIPLES OF THE INVENTION</u>

Growth in the use of plastic credit cards, and more recently debit cards and ATM cash cards, needs little introduction. Nor does there need to be much discussion here about the
10 long history of fraud and illicit uses of these financial instruments. The development of the credit card hologram, and its subsequent forgery development, nicely serves as a historic example of the give and take of plastic card security measures and fraudulent countermeasures. This section will concern itself with how the principles of this invention can be realized in an alternative, highly fraud-proof yet cost effective plastic card-based financial network.

15 A basic list of desired features for an ubiquitous plastic economy might be as follows: 1) A given plastic financial card is completely impossible to forge; 2) An attempted forged card (a "look-alike") cannot even function within a transaction setting; 3) Intercepted electronic transactions by a would-be thief would not in any way be useful or re-useable; 4) In the event of physical theft of an actual valid card, there are still formidable obstacles to a thief
20 using that card; and 5) The overall economic cost of implementation of the financial card network is equal to or less than that of the current international credit card networks, i.e., the fully loaded cost per transaction is equal to or less than the current norm, allowing for higher profit margins to the implementors of the networks. Apart from item 5, which would require a detailed analysis of the engineering and social issues involved with an all out implementation
25 strategy, the following use of the principles of this invention may well achieve the above list, even item 5.

Figures 1 through 5, along with the ensuing written material, collectively outline what is referred to in figure 5 as "The Negligible-Fraud Cash Card System." The reason that the fraud-prevention aspects of the system are highlighted in the title is that fraud, and the
30 concomitant lost revenue therefrom, is apparently a central problem in today's plastic card

based economies. The differential advantages and disadvantages of this system relative to current systems will be discussed after a preferred embodiment is presented.

Figure 1 illustrates the basic unforgeable plastic card which is quite unique to each and every user. A digital image 940 is taken of the user of the card. A computer, which is hooked into the central accounting network, 980, depicted in figure 5, receives the digital image 940, and after processing it (as will be described surrounding figure 3) produces a final rendered image which is then printed out onto the personal cash card 950. Also depicted in figure 1 is a straightforward identification marking, in this case a bar code 952, and optional position fiducials which may assist in simplifying the scanning tolerances on the Reader 958 depicted in figure 2.

The short story is that the personal cash card 950 actually contains a very large amount of information unique to that particular card. There are no magnetic strips involved, though the same principles can certainly be applied to magnetic strips, such as an implanted magnetic noise signal (see the February 8, 1994, Wall Street Journal, page B1, which discusses the use of very fine magnetic fluxuations on the magnetic strips of credit cards (fluxuations that tend to be unique from one card to the next) as a means of credit card authentication; here, the fingerprinting would be prominent and proactive as opposed to passive). In any event, the unique information within the image on the personal cash card 950 is stored along with the basic account information in a central accounting network, 980, figure 5. The basis for unbreakable security is that during transactions, the central network need only query a small fraction of the total information contained on the card, and never needs to query the same precise information on any two transactions. Hundreds if not thousands or even tens of thousands of unique and secure "transaction tokens" are contained within a single personal cash card. Would-be pirates who went so far as to pick off transmissions of either encrypted or even unencrypted transactions would find the information useless thereafter. This is in marked distinction to systems which have a single complex and complete "key" (generally encrypted) which needs to be accessed, in its entirety, over and over again. The personal cash card on the other hand contains thousands of separate and secure keys which can be used once, within milliseconds of time, then forever thrown away (as it were). The central network 980 keeps track of the keys and knows which have been used and which haven't.

Figure 2 depicts what a typical point-of-sale reading device, 958, might look like. Clearly, such a device would need to be manufacturable at costs well in line with, or cheaper than, current cash register systems, ATM systems, and credit card swipers. Not depicted in figure 2 are the innards of the optical scanning, image processing, and data communications

5   components, which would simply follow normal engineering design methods carrying out the functions that are to be described henceforth and are well within the capability of artisans in these fields. The reader 958 has a numeric punch pad 962 on it, showing that a normal personal identification number system can be combined with the overall design of this system adding one more conventional layer of security (generally after a theft of the physical card has

10   occurred). It should also be pointed out that the use of the picture of the user is another strong (and increasingly common) security feature intended to thwart after-theft and illicit use. Functional elements such as the optical window, 960, are shown, mimicking the shape of the card, doubling as a centering mechanism for the scanning. Also shown is the data line cable 966 presumably connected either to a proprietor's central merchant computer system or

15   possibly directly to the central network 980. Such a reader may also be attached directly to a cash register which performs the usual tallying of purchased items. Perhaps overkill on security would be the construction of the reader, 958, as a type of Faraday cage such that no electronic signals, such as the raw scan of the card, can emanate from the unit. The reader 958 does need to contain, preferably, digital signal processing units which will assist in swiftly

20   calculating the dot product operations described henceforth. It also should contain local read-only memory which stores a multitude of spatial patterns (the orthogonal patterns) which will be utilized in the "recognition" steps outlined in figure 4 and its discussion. As related in figure 2, a consumer using the plastic card merely places their card on the window to pay for a transaction. A user could choose for themselves if they want to use a PIN number or not.

25   Approval of the purchase would presumably happen within seconds, provided that the signal processing steps of figure 4 are properly implemented with effectively parallel digital processing hardware.

Figure 3 takes a brief look at one way to process the raw digital image, 940, of a user into an image with more useful information content and uniqueness. It should be clearly

30   pointed out that the raw digital image itself could in fact be used in the following methods, but

that placing in additional orthogonal patterns into the image can significantly increase the overall system. (Orthogonal means that, if a given pattern is multiplied by another orthogonal pattern, the resulting number is zero, where "multiplication of patterns" is meant in the sense of vector dot products; these are all familiar terms and concepts in the art of digital image

5   processing). Figure 3 shows that the computer 942 can, after interrogating the raw image 970, generate a master snowy image 972 which can be added to the raw image 970 to produce a yet-more unique image which is the image that is printed onto the actual personal cash card, 950. The overall effect on the image is to "texturize" the image. In the case of a cash card, invisibility of the master snowy pattern is not as much of a requirement as with commercial

10   imagery, and one of the only criteria for keeping the master snowy image somewhat lighter is to not obscure the image of the user. The central network, 980, stores the final processed image in the record of the account of the user, and it is this unique and securely kept image which is the carrier of the highly secure "throw-away transaction keys." This image will therefore be "made available" to all duly connected point-of-sale locations in the overall

15   network. As will be seen, none of the point-of-sale locations ever has knowledge of this image, they merely answer queries from the central network.

Figure 4 steps through a typical transaction sequence. The figure is laid out via indentations, where the first column are steps performed by the point-of-sale reading device 958, the second column has information transmission steps communicated over the data line

20   966, and the third column has steps taken by the central network 980 which has the secured information about the user's account and the user's unique personal cash card 950. Though there is some parallelism possible in the implementation of the steps, as is normally practiced in the engineering implementation of such systems, the steps are nevertheless laid out according to a general linear sequence of events.

25   Step one of figure 4 is the standard "scanning" of a personal cash card 950 within the optical window 960. This can be performed using linear optical sensors which scan the window, or via a two dimensional optical detector array such as a CCD. The resulting scan is digitized into a grey scale image and stored in an image frame memory buffer such as a "framegrabber," as is now common in the designs of optical imaging systems. Once the card

30   is scanned, a first image processing step would probably be locating the four fiducial center

points, 954, and using these four points to guide all further image processing operations (i.e. the four fiducials "register" the corresponding patterns and barcodes on the personal cash card). Next, the barcode ID number would be extracted using common barcode reading image processing methods. Generally, the user's account number would be determined in this step.

5   Step two of figure 4 is the optional typing in of the PIN number. Presumably most users would opt to have this feature, except those users who have a hard time remembering such things and who are convinced that no one will ever steal their cash card.

Step three of figure 4 entails connecting through a data line to the central accounting network and doing the usual communications handshaking as is common in modem-based

10   communications systems. The preferred embodiment of this system would obviate the need for standard phone lines, such as the use of optical fiber data links, but for now we can assume it is a garden variety belltone phone line and that the reader 958 hasn't forgotten the phone number of the central network.

After basic communications are established, step four shows that the point-of-sale

15   location transmits the ID number found in step 1, along with probably an encrypted version of the PIN number (for added security, such as using the ever more ubiquitous RSA encryption methods), and appends the basic information on the merchant who operates the point-of-sale reader 958, and the amount of the requested transaction in monetary units.

Step five has the central network reading the ID number, routing the information

20   accordingly to the actual memory location of that user's account, thereafter verifying the PIN number and checking that the account balance is sufficient to cover the transaction. Along the way, the central network also accesses the merchant's account, checks that it is valid, and readies it for an anticipated credit.

Step six begins with the assumption that step five passed all counts. If step five didn't,

25   the exit step of sending a NOT OK back to the merchant is not depicted. So, if everything checks out, the central network generates twenty four sets of sixteen numbers, where all numbers are mutually exclusive, and in general, there will be a large but quite definitely finite range of numbers to choose from. Figure 4 posits the range being 64K or 65536 numbers. It can be any practical number, actually. Thus, set one of the twenty four sets might have the

30   numbers 23199, 54142, 11007, 2854, 61932, 32879, 38128, 48107, 65192, 522, 55723,

27833, 19284, 39970, 19307, and 41090, for example. The next set would be similarly random, but the numbers of set one would be off limits now, and so on through the twenty four sets. Thus, the central network would send (16x24x2 bytes) of numbers or 768 bytes. The actual amount of numbers can be determined by engineering optimization of security

5   versus transmission speed issues. These random numbers are actually indexes to a set of 64K universally *a priori* defined orthogonal patterns which are well known to both the central network and are permanently stored in memory in all of the point-of-sale readers. As will be seen, a would-be thief's knowledge of these patterns is of no use.

Step seven then transmits the basic "OK to proceed" message to the reader, 958, and

10   also sends the 24 sets of 16 random index numbers.

Step eight has the reader receiving and storing all these numbers. Then the reader, using its local microprocessor and custom designed high speed digital signal processing circuitry, steps through all twenty four sets of numbers with the intention of deriving 24 distinct floating point numbers which it will send back to the central network as a "one time

15   key" against which the central network will check the veracity of the card's image. The reader does this by first adding together the sixteen patterns indexed by the sixteen random numbers of a given set, and then performing a common dot product operation between the resulting composite pattern and the scanned image of the card. The dot product generates a single number (which for simplicity we can call a floating point number). The reader steps

20   through all twenty four sets in like fashion, generating a unique string of twenty four floating point numbers.

Step nine then has the reader transmitting these results back to the central network.

Step ten then has the central network performing a check on these returned twenty four numbers, presumably doing its own exact same calculations on the stored image of the card

25   that the central network has in its own memory. The numbers sent by the reader can be "normalized," meaning that the highest absolute value of the collective twenty four dot products can divided by itself (its unsigned value), so that brightness scale issues are removed. The resulting match between the returned values and the central network's calculated values will either be well within given tolerances if the card is valid, and way off if the card is a

30   phony or if the card is a crude reproduction.

Step eleven then has the central network sending word whether or not the transaction was OK, and letting the customer know that they can go home with their purchased goods.

Step twelve then explicitly shows how the merchant's account is credited with the transaction amount.

5   As already stated, the primary advantage of this plastic card invention is to significantly reduce fraud, which apparently is a large cost to current systems. This system reduces the possibility of fraud only to those cases where the physical card is either stolen or very carefully copied. In both of these cases, there still remains the PIN security and the user picture security (a known higher security than low wage clerks analyzing signatures).

10   Attempts to copy the card must be performed through "temporary theft" of the card, and require photo-quality copying devices, not simple magnetic card swipers. The system is founded upon a modern 24 hour highly linked data network. Illicit monitoring of transactions does the monitoring party no use whether the transmissions are encrypted or not.

It will be appreciated that the foregoing approach to increasing the security of

15   transactions involving credit and debit card systems is readily extended to any photograph-based identification system. Moreover, the principles of the present invention may be applied to detect alteration of photo ID documents, and to generally enhance the confidence and security of such systems. In this regard, reference is made to Fig. 6, which depicts a photo-ID card or document 1000 which may be, for example, a passport or visa, driver's license, credit

20   card, government employee identification, or a private industry identification badge. For convenience, such photograph-based identification documents will be collectively referred to as photo ID documents.

The photo ID document includes a photograph 1010 that is attached to the document 1000. Printed, human-readable information 1012 is incorporated in the document 1000,

25   adjacent to the photograph 1010. Machine readable information, such as that known as "bar code" may also be included adjacent to the photograph.

Generally, the photo ID document is constructed so that tampering with the document (for example, swapping the original photograph with another) should cause noticeable damage to the card. Nevertheless, skilled forgerers are able to either alter existing documents or

30   manufacture fraudulent photo ID documents in a manner that is extremely difficult to detect.

As noted above, the present invention enhances the security associated with the use of photo ID documents by supplementing the photographic image with encoded information (which information may or may not be visually perceptible), thereby facilitating the correlation of the photographic image with other information concerning the person, such as the printed information 1012 appearing on the document 1000.

In one embodiment of this aspect of the invention, the photograph 1010 may be produced from a raw digital image to which is added a master snowy image as described above in connection with Figs. 1-3. The above-described central network and point-of-sale reading device (which device, in the present embodiment, may be considered as a point-of-entry or point-of-security photo ID reading device), would essentially carry out the same processing as described with that embodiment, including the central network generation of unique numbers to serve as indices to a set of defined orthogonal patterns, the associated dot product operation carried out by the reader, and the comparison with a similar operation carried out by the central network. If the numbers generated from the dot product operation carried out by the reader and the central network match, in this embodiment, the network sends the OK to the reader, indicating a legitimate or unaltered photo ID document.

In another embodiment of this aspect of the invention, the photograph component 1010 of the identification document 1000 may be digitized and processed so that the photographic image that is incorporated into the photo ID document 1000 corresponds to the "distributable signal" as defined above. In this instance, therefore, the photograph includes a composite, embedded code signal, imperceptible to a viewer, but carrying an N-bit identification code. It will be appreciated that the identification code can be extracted from the photo using any of the decoding techniques described above, and employing either universal or custom codes, depending upon the level of security sought.

It will be appreciated that the information encoded into the photograph may correlate to, or be redundant with, the readable information 1012 appearing on the document. Accordingly, such a document could be authenticated by placing the photo ID document on a scanning system, such as would be available at a passport or visa control point. The local computer, which may be provided with the universal code for extracting the identification information, displays the extracted information on the local computer screen so that the

operator is able to confirm the correlation between the encoded information and the readable information 1012 carried on the document.

It will be appreciated that the information encoded with the photograph need not necessarily correlate with other information on an identification document. For example, the

5   scanning system may need only to confirm the existence of the identification code so that the user may be provided with a "go" or "no go" indication of whether the photograph has been tampered with. It will also be appreciated that the local computer, using an encrypted digital communications line, could send a packet of information to a central verification facility, which thereafter returns an encrypted "go" or "no go" indication.

10   In another embodiment of the present invention, it is contemplated that the identification code embedded in the photograph may be a robust digital image of biometric data, such as a fingerprint of the card bearer, which image, after scanning and display, may be employed for comparison with the actual fingerprint of the bearer in very high security access points where on-the-spot fingerprint recognition systems (or retinal scans, etc.) are employed.

15   It will be appreciated that the information embedded in the photograph need not be visually hidden or steganographically embedded. For example, the photograph incorporated into the identification card may be a composite of an image of the individual and one-, or two-dimensional bar codes. The bar code information would be subject to conventional optical scanning techniques (including internal cross checks) so that the information derived from the

20   code may be compared, for example, to the information printed on the identification document.

It is also contemplated that the photographs of ID documents currently in use may be processed so that information correlated to the individual whose image appears in the photograph may be embedded. In this regard, the reader's attention is directed to the

25   foregoing portion of this description entitled "Use in Printing, Paper, Documents, Plastic-Coated Identification Cards, and Other Material Where Global Embedded Codes Can Be Imprinted," wherein there is described numerous approaches to modulation of physical media that may be treated as "signals" amenable to application of the present invention principles.

Claims

I CLAIM:

1. A security document comprising:

a substrate;

text printed on the substrate;

a graphic carried by the substrate, the graphic conveying a visual impression to human viewers thereof;

the graphic additionally being steganographically encoded to secretly convey plural bits of digital data recoverable by computer analysis of said graphic;

wherein the printed text and the steganographically encoded plural bits of digital data cooperate to verify authenticity of the security document.

2. The document of claim 1 in which the graphic is an image.

3. The document of claim 2 in which the image is a photographic image..

4. The document of claim 1 wherein said digital data corresponds to at least part of said printed text.

5. The document of claim 1 wherein said digital data serves as an index into a registry containing additional information.

6. The document of claim 1 wherein said steganographic encoding does not visibly interrupt said graphic.

7. The document of claim 1 wherein said steganographic encoding adds noise to the graphic, said noise not being perceptible as a representation of said plural-bit digital data except by computer analysis, wherein the encoded graphic does not appear to convey digital data to human viewers thereof.

SECURITY DOCUMENT WITH STEGANOGRAPHICALLY-ENCODED AUTHENTICATION DATA

Abstract of the Disclosure

5　　　　Security of a document is enhanced by steganographically embedding, within a graphic on the document, data that can be used in conjunction with text on the document to authenticate the document.

FIG. 1

DIGITAL IMAGE TAKEN
OF CUSTOMER

940

942

COMPUTER
PROCESSES NEW
ENCODED IMAGE

PRINTS
PROCESSED
IMAGE ONTO
PLASTIC CARD

952

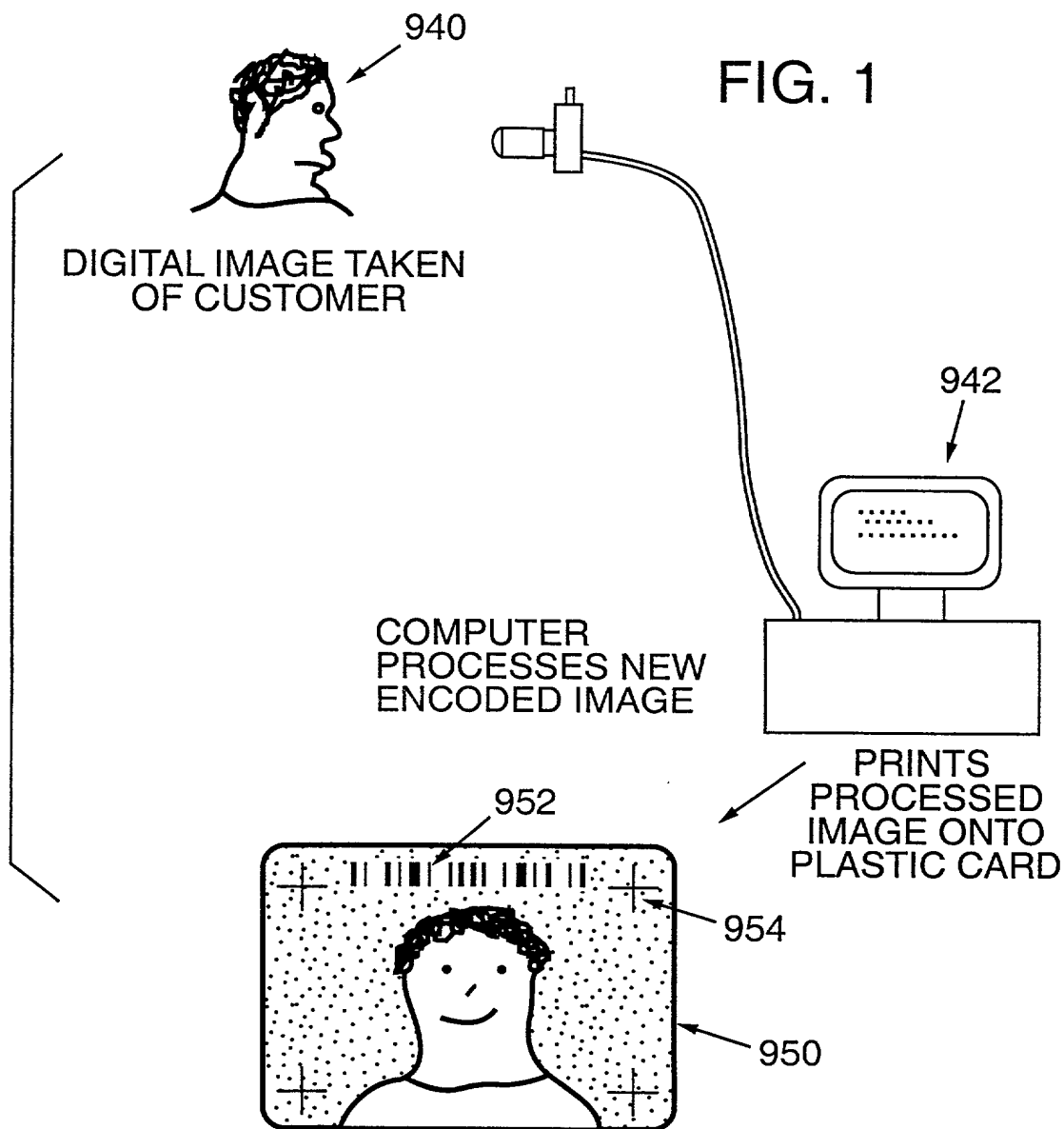954

950

FIG. 2

CABLE, 964,
TO DATA LINE,
966

960

962

958
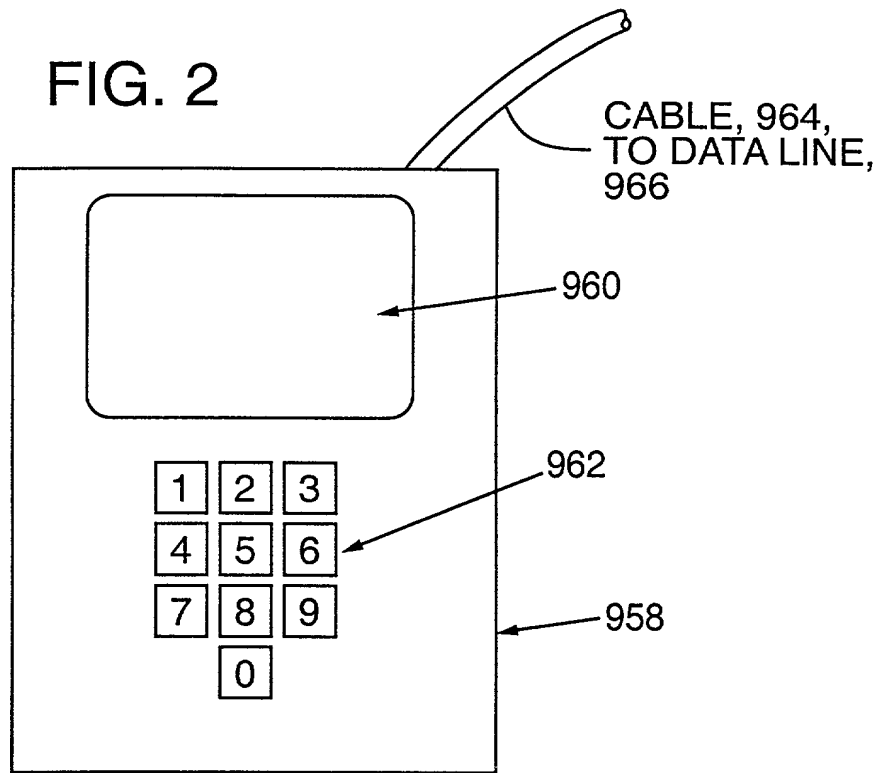
CONTAINS RUDIMENTARY OPTICAL SCANNER,
MEMORY BUFFERS, COMMUNICATIONS DEVICES,
AND MICROPROCESSOR

CONSUMER MERELY PLACES CARD INTO WINDOW
AND CAN, AT THEIR PREARRANGED OPTION, EITHER
TYPE IN A PERSONAL IDENTIFICATION NUMBER
(PIN, FOR ADDED SECURITY) OR NOT. THE TRANSACTION
IS APPROVED OR DISAPPROVED WITHIN SECONDS.

FIG. 3

ORIGINAL DIGITAL IMAGE WITH BARCODE AND FIDUCIALS ADDED

COMPUTER GENERATES MASTER SNOWY IMAGE WHICH IS GENERALLY ORTHOGONAL TO ORIGINAL IMAGE AT LEFT
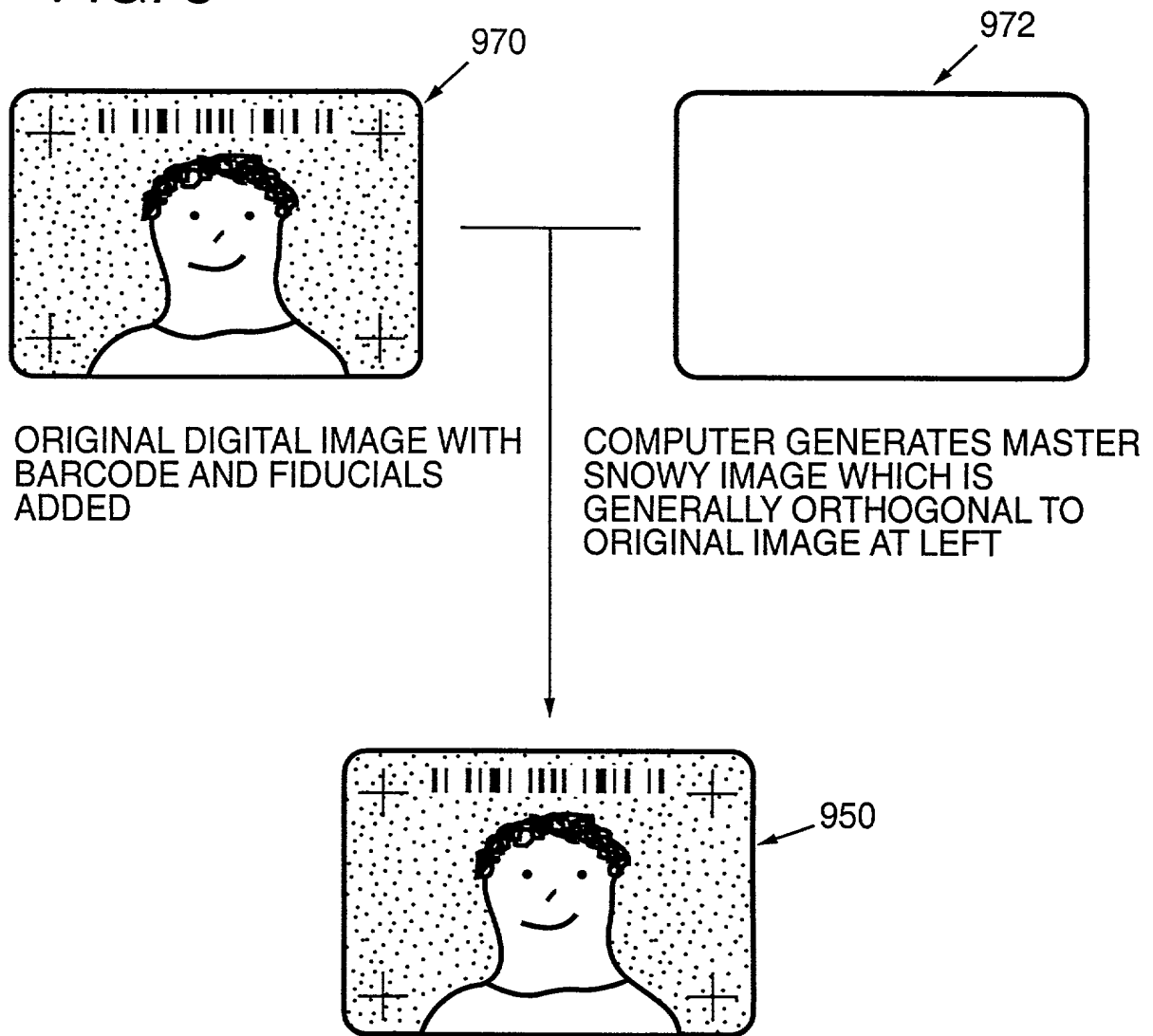
COMBINED TO FORM PERSONAL CASH CARD

FIG. 4

Typical Transaction Steps

Reader scans images on card; stores in memory; extracts person's ID. (Optional: user keys in PIN number) — 1

↓

Optional: User keys in PIN number — 2

↓

Reader calls central account data network; handshakes — 3

↓

Reader sends ID, (PIN), merchant information, and requested transaction amount to central network — 4

↓

Central Network verifies ID, PIN, Merchant info, and account balance — 5

↓

If OK, Central Network generates twenty four sets of sixteen distinct random numbers, where the random numbers are indexes to a set of 64K orthogonal spatial patterns — 6

↓

Central Network transmits first OK, and the sets of random numbers — 7

↓

Reader steps through the twenty four sets — 8

↓

Reader Adds together set of orthogonal patterns — 8A

↓

Reader performs dot product of resultant pattern and card scan; stores result — 8B

↓

Reader transmits the twenty four dot product results to Central Network — 9

↓

Central Network checks results against master — 10

↓

Central Network sends final approval or denial — 11

↓

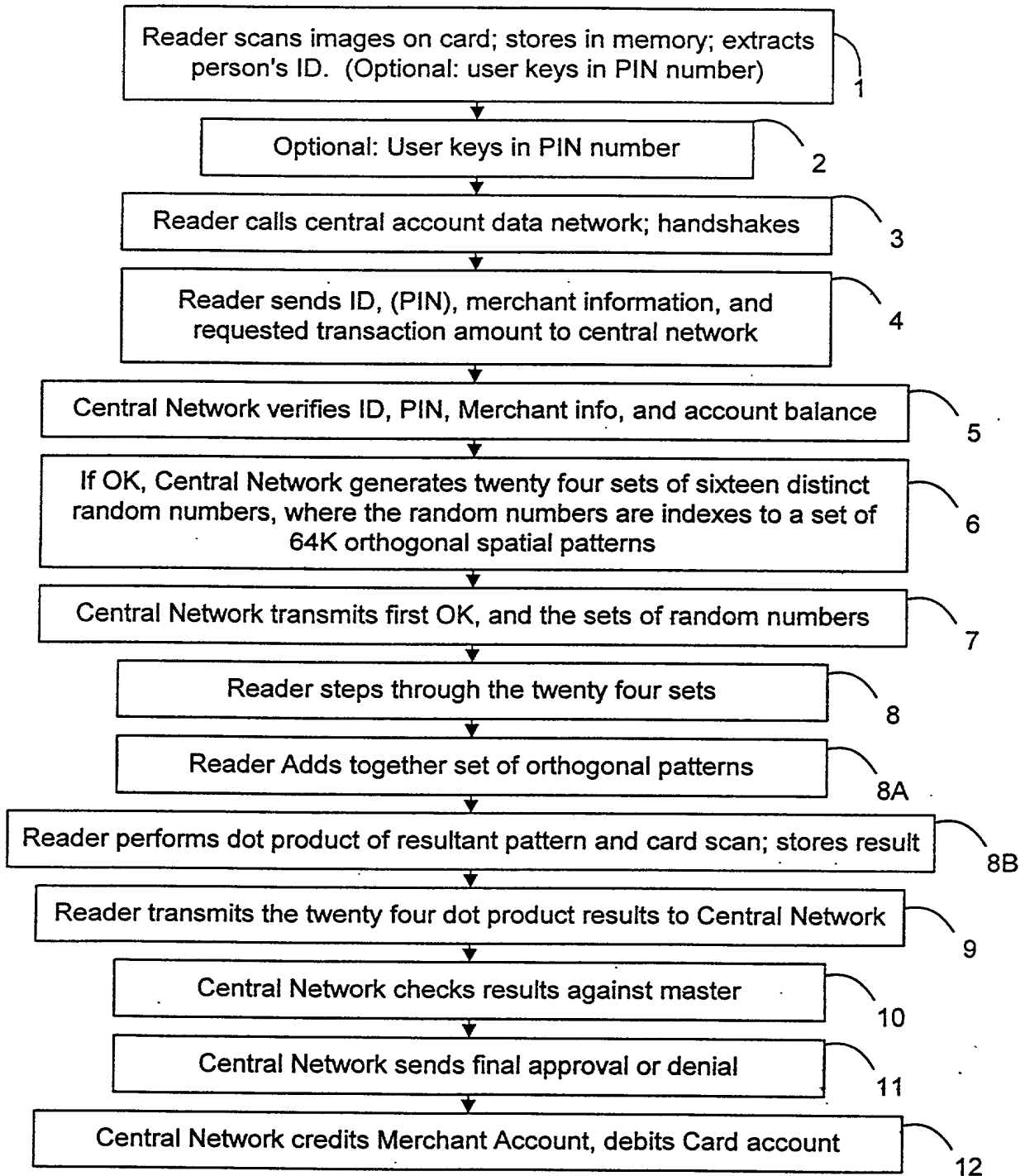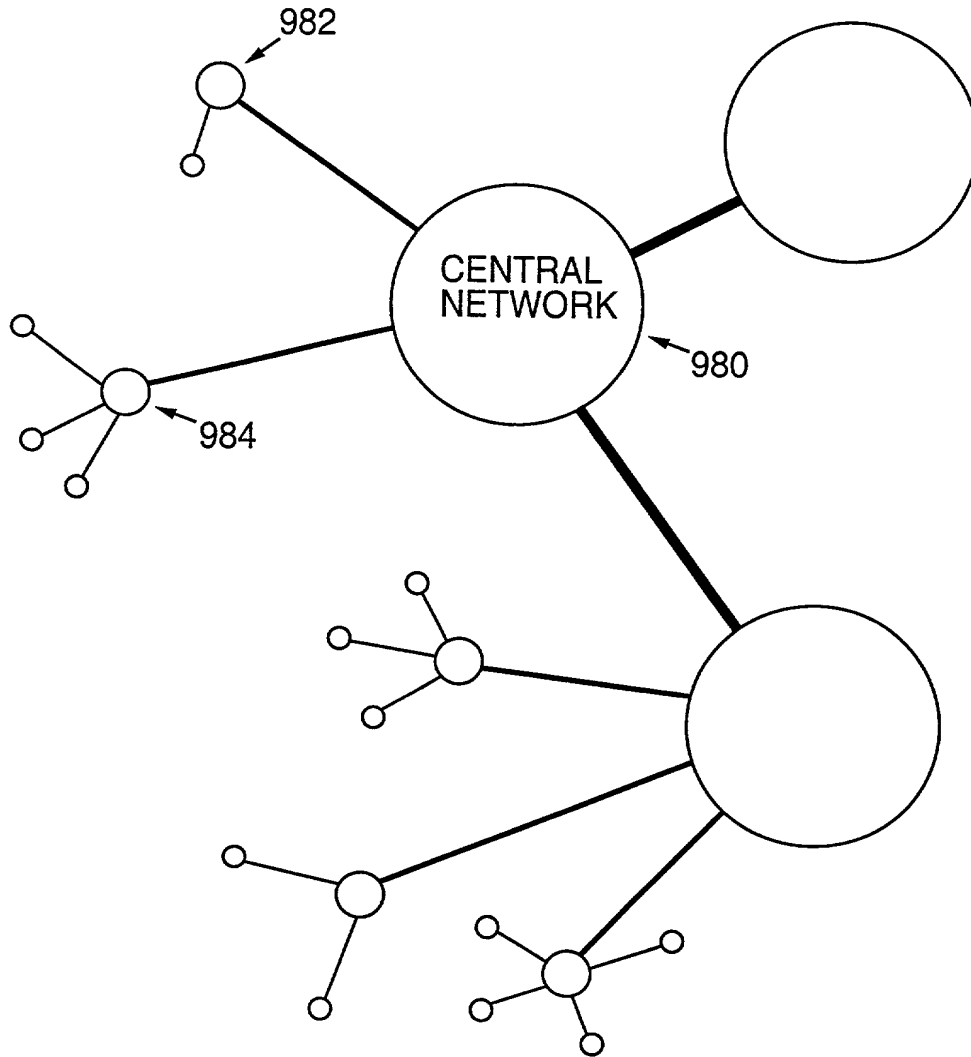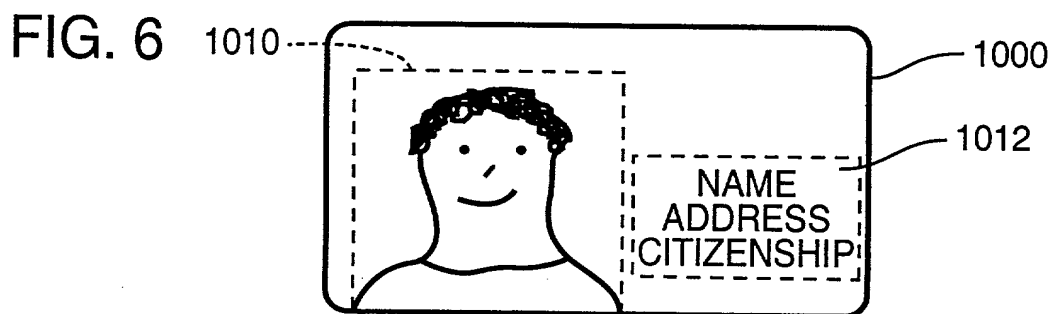Central Network credits Merchant Account, debits Card account — 12

FIG. 5

THE NEGLIGIBLE-FRAUD CASH CARD SYSTEM

A BASIC FOUNDATION OF THE CASH CARD SYSTEM IS A 24-HOUR
INFORMATION NETWORK, WHERE BOTH THE STATIONS WHICH CREATE
THE PHYSICAL CASH CARDS, 950, AND THE POINT-OF-SALES, 984,
ARE ALL HOOKED UP TO THE SAME NETWORK CONTINUOUSLY

FIG. 6

COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled SECURITY SYSTEM FOR PHOTOGRAPHIC IDENTIFICATION, the specification of which

[X] is attached hereto.

[ ] was filed on _____ as Application Serial No. _____.

[ ] and was amended on _____ (if applicable).

[ ] with amendments through _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a). If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. §120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)   Priority
                                                     Claimed

                                                     [ ]   [ ]
_____   _____   Yes   No
(Number)   (Country)   (Day/Month/Year Filed)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____   _____   _____
(Application Serial No.) (Filing Date)   (Status: patented,
                                          pending, abandoned)

The undersigned hereby authorizes the U.S. attorney or agent named herein to accept and follow instructions from _____ as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney or agent and the undersigned. In

the event of a change in the persons from whom instructions may be taken, the U.S. attorney or agent named herein will be so notified by the undersigned.

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith:

Name	Reg. No.	Name	Reg. No.
Kenneth S. Klarquist	16,445	John W. Stuart	24,540
James Campbell	19,978	Donald L. Stephens Jr.	34,022
James S. Leigh	20,434	Stacey C. Slater	36,011
Arthur L. Whinston	19,155	Douglas D. Hancock	35,889
David P. Petersen	28,106	Garth A. Winn	33,220
Richard J. Polley	28,107	Stephen A. Wight	37,759
Ramon A. Klitzke II	30,188	Joel R. Meyer	37,677
William Y. Conwell	31,943	Joseph T. Jakubek	34,190
Mark L. Becker	31,325	Mark A. Porter	35,327
William D. Noonan	30,878	Timothy M. Carlson	38,095
John D. Vandenberg	31,312	Alan E. Dow	35,123
Patrick W. Hughey	31,169	Mark M. Meininger	32,428

Address all telephone calls to William Y. Conwell at telephone number (503) 226-7391.

Address all correspondence to:

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: Geoffrey B. Rhoads

Inventor's signature X _____ X 8-9-95
                                                                                    Date

Residence: West Linn, Oregon

Citizenship: United States of America

Post Office address: 363 SW Tualatin Loop
                                West Linn, Oregon 97068